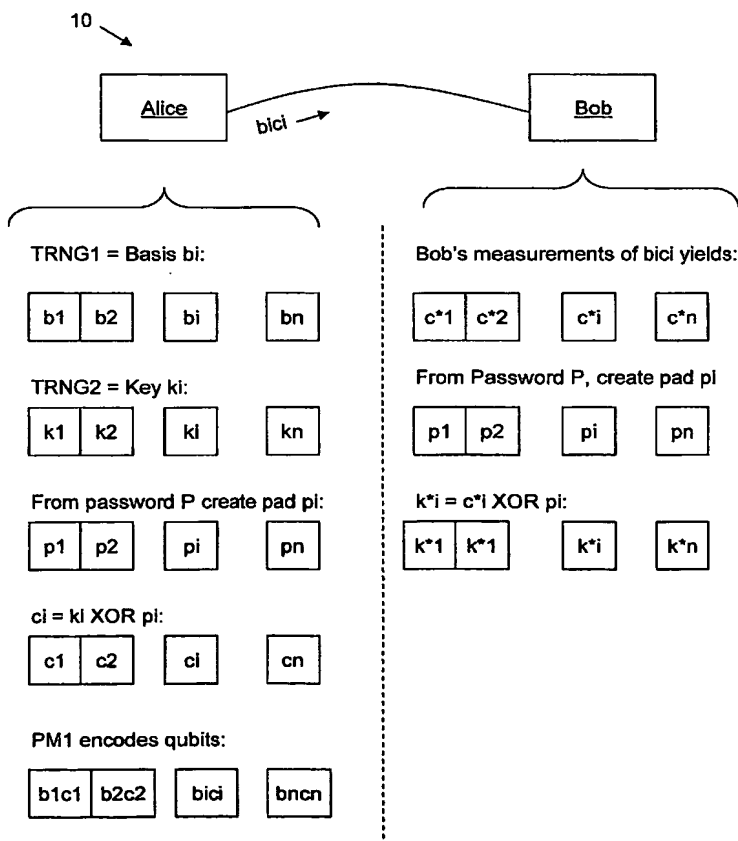(72) Inventors; and
(75) Inventors/Applicants (for US only): BERZANSKIS, Audrius [LT/US]; 7 Saint Mary Road, Cambridge, MA 02139 (US). YOUNG, Jonathan [US/US]; 145 State Street, Newburyport, MA 01950 (US).

(74) Agent: GORTYCH, Joseph, E.; MagiQ Technologies, Inc., 171 Madison Avenue, Suite 1300, New York, NY 10016 (US).

(54) Title: QKD WITH CLASSICAL BIT ENCRYPTION

(57) Abstract: A method for enhancing the security of a quantum key distribution (QKD) system having QKD stations Alice and Bob (10) is disclosed. The method includes encrypting key bits generated by a random number generator and sent to a polarization or phase modulator to encode weak optical pulses as qubits to be shared between Alice and Bob (10). Key bit encryption is achieved by using shared password and a stream cipher. Bob obtains at least a subset of the original key bits used by Alice (10) by utilizing the same cipher stream and the shared password.

Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.